Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

OCA 86-1931
9 June 1986

STAT MEMORANDUM FOR: [redacted]
Intelligence Law Division, OGC

STAT FROM: [redacted]
Legislation Division
Office of Congressional Affairs

SUBJECT: Update on Computer Security Legislation

1. On 4 June 1986, the House Science and Technology Committee marked up and unanimously reported out H.R. 2889, the Computer Security Act of 1986. The version adopted by Science and Technology was a substitute amendment offered by Congressman Glickman to the version originally reported out by a subcommittee of House Science and Technology. I have attached for your review a copy of the bill, an explanation of the Committee print of H.R. 2889, and statements for the record read by Congressmen Brown and Boehlert at the markup. The version adopted by Science and Technology must now be reconciled with the version of the bill adopted by the House Government Operations Committee. Following reconciliation of the different versions of the same bill, a clean bill may be introduced and sent to the House floor.

2. NSA continues to oppose the bill and is formulating a position paper to be given to the Armed Services Committee outlining the reasons why they should take a sequential referral. The prospects for a referral are not as bright as they were last December because the version of the bill reported out of Science and Technology has been modified enough that DOD equities are not as severely affected as they were under the House Government Operations' version of the bill. NSA strategy continues to be one of delay in the hope that time will run out before Congress can enact this bill.

3. As you recall, the only part of the bill of possible concern to this Agency is Section 6. While that section does not have an explicit provision in it excluding Agency computers, the reference in the section to guidelines developed under the Federal Property and Administrative Services Act which we are exempt from should provide the legal reasoning for us to argue that we are exempt from this section as well.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

4. My recommendation is to continue to let NSA take the lead in opposing the bill. While it would be "frosting on the cake" for the Agency to get an explicit exemption to Section 6, OMB has stated that they do not want the Agency to further improve the bill from the standpoint of the Intelligence Community for fear that it will then make it even more difficult for the Administration to oppose the bill in its entirety. I, therefore, do not believe we should attempt to get an explicit exemption for the Agency through a floor amendment. However, a Republican minority staff person, Maryanne Bach, on House Science and Technology has stated that they would be willing to insert some legislative history in the Minority Statement on the bill defining the scope of Section 6. Ms. Bach has requested that the Agency draft the legislative history and provide it to her in the next couple of days. Attached is a draft of the legislative history that I prepared. The only possible drawback of providing this legislative history to her is that the Majority Staff may draft counter-legislative history to ensure that CIA is covered by the section. Unless this legislative history is carefully inserted into the record, our attempts to clarify the scope of the bill could boomrang. I welcome the views of ILD on whether, from OGC's perspective, we should attempt to further clarify the scope of Section 6. I will also continue to monitor progress of the bill to ensure that any compromise between Science and Technology and Government Operations will not impact on the Agency.

STAT [redacted]

Attachments as
stated

Distribution:
Original - Addressee
1 - D/OCA
1 - ExO/OCA
1 - OCA Registry
1 - DMP/Signer
1 - OCA/LEG Subject File: Computer Fraud

STAT OCA/LEG/[redacted]:pap (9 June 1986)

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Explanation of Committee Print
of
H.R. 2889 - Computer Security Act of 1986

The following explanation was prepared by Committee staff after staff completed its discussions following the actions of the TAM and SRT Subcommittees. The revised version reflects the following overall concepts:

1. establish a civilian authority for developing computer security standards relating to unclassified information;

2. institute a program of mandatory training for federal employees in computer security awareness;

3. protect the ongoing missions of NBS by providing for a separate appropriation for computer security; and

4. affirm the Science Committee jurisdiction over NBS by including all functions to be conducted by NBS in an amendment to its basic Act and removing those functions from other portions of the bill.

In drafting the bill to reflect these concepts and to simplify the language,

1. emphasis is placed on protecting information rather than computer systems in the sections relating to security;

2. the term "computer system" is used throughout to include data communications;

3. the term "federal computer system" is used to define the reach of the bill to include federal agencies, their contractors and others, such as state agencies, that process information for the federal government;

4. with regard to computer security standards, mandatory training and security plans, the bill applies only to sensitive (unclassified) information;

5. the bill exempts intelligence, crypotologic, command and control, and other systems critical to military missions (Warner amendment systems), both classified and unclassified;

6. with regard to computer standards, other than for security, the bill applies only to Brooks Act systems;

7. the bill amends the NBS Act to provide a statutory basis for its work in computers, generally;

8. the bill provides flexibility to NBS to recommend the extent to which computer standards should be made mandatory;

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

9. the bill retains the Advisory Board as a means to generate visibility and greater awareness of computer security problems and to provide a civilian counterpart to the structure created by NSDD-145;

10. the bill places the responsibility for actual issuance of standards with the Secretary of Commerce;

11. the bill provides a mechanism for waiving standards when conditions justify such action.

12. the bill provides a mechanism for agencies, employing computer security provisions that are more stringent than NBS' standards, to use those provisions in lieu of NBS standards.

ACT/wm
May 21, 1986

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

HONORABLE GEORGE E. BROWN, JR., CHAIRMAN
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE AND TECHNOLOGY

JUNE 4, 1986

H.R. 2889, THE COMPUTER SECURITY RESEARCH & TRAINING ACT

MR. CHAIRMAN. THE NEED FOR H.R. 2889 WAS IDENTIFIED IN HEARINGS, HELD JUST ABOUT ONE YEAR AND A HALF AGO BEFORE THE TRANSPORTATION, AVIATION AND MATERIALS SUBCOMMITTEE. AT THAT TIME, WE NOTED THAT THE FEDERAL GOVERNMENT HAD BECOME TOTALLY DEPENDENT ON AUTOMATED INFORMATION SYSTEMS TO PERFORM A MULTITUDE OF ESSENTIAL SERVICES. FURTHERMORE, THE INFORMATION STORED IN GOVERNMENT COMPUTERS AND TRANSMITTED OVER VARIOUS COMMUNICATIONS NETWORKS IS VULNERABLE TO UNAUTHORIZED ACCESS AND DISCLOSURE, FRAUDULENT MANIPULATION, AND DISRUPTION. THE SITUATION WAS DESCRIBED AS THE ELECTRONIC EQUIVALENT OF LEAVING THE BANK DOOR UNLOCKED.

YET, DESPITE THE POTENTIAL SERIOUS CONSEQUENCES OF THESE THREATS, WE FOUND LITTLE EVIDENCE OF AN OVERALL, SYSTEMATIC APPROACH TO COMPUTER AND COMMUNICATIONS SECURITY.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

OF PARTICULAR CONCERN WAS THE LEVEL OF SECURITY AMONG PEOPLE WHO OPERATE, USE AND MANAGE COMPUTERS. SUCH PEOPLE ARE EXTREMELY IMPORTANT IN A SECURITY SENSE BECAUSE, AS STUDIES HAVE SHOWN, THEY ARE THE GREATEST PROBLEM. IT IS NOT THE MUCH-PUBLICIZED HACKER, WORKING TO PENETRATE FROM THE OUTSIDE. RATHER, IT IS THE INSIDER, THE ONE WHO ALREADY HAS AUTHORIZED ACCESS, THAT CAUSES THE GREATEST DAMAGE, IN PRACTICE.

YET, AS WE LEARNED FROM GAO'S SURVEY OF 25 COMPUTER SYSTEMS, THERE IS VERY LITTLE FORMALIZED EFFORT MADE TO REACH THESE INDIVIDUALS, TO MAKE THEM AWARE OF SYSTEM VULNERABILITIES AND THE IMPORTANCE OF ENHANCING SECURITY.

THE PURPOSE OF H.R. 2889, AS INTRODUCED, IS TO STRENGTHEN THIS WEAK LINK. IT DOES THIS BY ESTABLISHING A RESEARCH PROGRAM AT THE NATIONAL BUREAU OF STANDARDS AIMED AT DEVELOPING GUIDANCE FOR USE BY AGENCIES IN STRUCTURING COMPUTER SECURITY AWARENESS TRAINING PROGRAMS FOR THEIR EMPLOYEES. IT ALSO MAKES IT MANDATORY THAT SUCH TRAINING BE GIVEN PERIODICALLY IN EACH AGENCY.

THE BILL WAS REFERRED JOINTLY TO THE COMMITTEES ON SCIENCE AND TECHNOLOGY, AND GOVERNMENT OPERATIONS. GOVERNMENT OPERATIONS COMPLETED ITS MARKUP LAST FALL, MAKING SUBSTANTIAL CHANGES TO THE SCOPE OF THE BILL.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

TO UNDERSTAND THOSE CHANGES, IT IS NECESSARY TO REVIEW BRIEFLY A RELATED, BUT SEPARATE ACTION -- KNOWN AS NATIONAL SECURITY DECISION DIRECTIVE 145 -- TAKEN BY THE PRESIDENT ABOUT A YEAR AND A HALF AGO. NSDD-145 IS A LONG-OVERDUE STEP TO CREATE A FOCUS FOR COMPUTER SECURITY IN THE FEDERAL GOVERNMENT. IT SETS UP AN INTERAGENCY COMMITTEE TO DEAL BROADLY WITH GOVERNMENT COMPUTER SECURITY PROBLEMS BY ISSUING STANDARDS AND GUIDELINES THAT WILL APPLY GOVERNMENT-WIDE.

THE CONCEPT IS A GOOD ONE. VIRTUALLY EVERYONE RECOGNIZES THAT BETTER CENTRALIZED LEADERSHIP IS NEEDED. BUT THE PARTICULAR FORMULA IN NSDD-145, WHICH HEAVILY FAVORS THE MILITARY, IS VIEWED WITH CONCERN BY SOME CIVIL AGENCIES AND BY OTHERS WHO SEE A POTENTIAL THREAT TO OPENNESS IN GOVERNMENT. THESE CONCERNS WERE VOICED LAST SUMMER DURING OUR HEARING ON NSDD-145, AT WHICH MR. BROOKS WAS A WITNESS.

SUBSEQUENTLY, THE GOVERNMENT OPERATIONS COMMITTEE BROADENED H.R. 2889 SUBSTANTIALLY TO PROVIDE A CIVIL ALTERNATIVE (HOUSED AT NBS) TO THE COMMITTEE CREATED BY NSDD-145. IT ALSO ADDED AN ADVISORY BOARD TO ASSURE THE VIEWS OF THE PRIVATE SECTOR ARE CONSIDERED BY NBS IN DEVELOPING COMPUTER SECURITY STANDARDS.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

THE VERSION OF H.R. 2889 REPORTED BY TAM RETAINS THE TRAINING PROVISIONS OF THE ORIGINAL BILL AND THE ESSENTIAL FEATURES ADDED BY GOVERNMENT OPERATIONS. IN ADDITION, THE SUBCOMMITTEE ADDED SEVERAL AMENDMENTS TO CLARIFY THE NBS ROLE AND EXTEND THE COVERAGE OF THE BILL TO INCLUDE ORGANIZATIONS THAT ADMINISTER FEDERAL PROGRAMS, SUCH AS STATE AGENCIES.

EACH MEMBER HAS BEFORE HIM OR HER A COPY OF THE SUBCOMMITTEE REPORT WHICH EXPLAINS IN MORE DETAIL THE ADDITIONS MADE BY TAM. IF MEMBERS HAVE QUESTIONS ON THIS OR THE BILL, I SHALL BE GLAD TO TRY TO ANSWER THEM.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

OPENING STATEMENT

BY

HON. SHERWOOD BOEHLERT (R-NY)

JUNE 4, 1986

H.R. 2889, THE COMPUTER SECURITY ACT OF 1986

MR. CHAIRMAN:

ON NOVEMBER 21, 1985, THE COMMITTEE MET TO MARKUP H.R. 2889, THE COMPUTER SECURITY ACT. AT THAT TIME, CONGRESSMAN LUJAN AND I RAISED SEVERAL ISSUES STILL UNRESOLVED IN THE LEGISLATION. THESE DIFFERENCES REFLECT CHANGES WHICH HAD OCCURED DURING THE GOVERNMENT OPERATIONS COMMITTEE CONSIDERATION OF THE BILL. THE PRODUCT OF THEIR MARKUP RESULTED IN LEGISLATION QUITE UNLIKE THAT ORIGINALLY INTRODUCED BY MR. GLICKMAN.

AN AGREEMENT IN PRINCIPLE WAS MADE AT THE NOVEMBER 21 MARKUP THAT THE STAFF OF SRT, TAM, AND FULL COMMITTEE WOULD WORK TO RESOLVE THE DIFFERENCES BETWEEN THE RANKING REPUBLICAN MEMBERS AND THE MAJORITY. WHAT IS BEFORE US TODAY IS THE CULMINATION OF THAT AGREEMENT.

THE SUBSTITUTE AMENDMENT (COMMITTEE PRINT) ASSIGNS TO THE NATIONAL BUREAU OF STANDARDS RESPONSIBILITY FOR ESTABLISHING STANDARDS AND GUIDELINES FOR FEDERAL COMPUTER SYSTEMS THAT FALL UNDER THE BROOKS ACT (I.E. THE FEDERAL PROPERTY AND

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

ADMINISTRATIVE SERVICES ACT OF 1949, FOR AUTOMATIVE DATA PROCESSING SYSTEMS IN THE CIVILIAN AGENCIES). THERE ARE NUMEROUS COMPUTER SYSTEMS, HOWEVER, THAT ARE DESIGNATED AS "SENSITIVE" BUT NON CLASSIFIED. THIS IS HANDLED IN TWO WAYS UNDER THE SUBSTITUTE AMENDMENT. FIRST, SEC. 6 DEFINES THE TERM "SENSITIVE INFORMATION" FOR THE PURPOSES OF THIS BILL. SECONDLY, SEC. 4 GIVES AUTHORITY TO THE HEAD OF EACH FEDERAL AGENCY TO EMPLOY MORE STRINGENT STANDARDS THAN THOSE DEVELOPED BY NBS. THIS PROVISION ASSURES THAT AN AGENCY WOULD NOT BE BURDENED WITH TWO DIFFERENT SETS OF STANDARDS IF, IN FACT, THE AGENCY FELT STRICTER STANDARDS WERE NECESSARY, OR IF THE COMPUTER SYSTEM WAS USED FOR BOTH CLASSIFIED AND UNCLASSIFIED PURPOSES.

ANOTHER IMPORTANT CHANGE MADE IN THE BILL IS THAT IT RECOGNIZES UNDER SEC. (2)(B)(1) THAT NBS, WHILE HAVING RESPONSIBILITY FOR THE PURPOSES OF THIS ACT, DOES NOT CONFLICT WITH THE ROLE OF THE NATIONAL SECURITY AGENCY, WHICH IS RESPONSIBLE FOR STANDARDS ON CLASSIFIED COMPUTER SYSTEMS. IN FACT, IT IS THE INTENT OF THIS LEGISLATION, AS DISCUSSED BY MEMBERS AND DURING MEETINGS OF THE SUBCOMMITTEES, THAT TO THE EXTENT APPROPRIATE, THESE TWO AGENCIES SHOULD KEEP ABREAST OF DEVELOPMENTS IN COMPUTER SECURITY STANDARDS EACH AGENCY IS WORKING ON.

FINALLY, THE BILL DELEGATES TO THE OFFICE OF MANAGEMENT AND BUDGET (OMB), WITH THE ASSISTANCE OF NBS, THE ROLE OF DEVELOPING REGULATIONS PERTAINING TO THE TRAINING OF CIVILIAN FEDERAL

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

COMPUTER SYSTEM OPERATORS.

AFTER LONG DELIBERATION, I BELIEVE GREAT PROGRESS HAS BEEN MADE TOWARD A BILL WHICH THE COMMITTEE CAN APPROVE TO BE REPORTED. I URGE MEMBERS TO SUPPORT THIS VERSION OF THE BILL AS THE BEST POSSIBLE PRODUCT.

ONCE REPORTED, THE SCIENCE AND TECHNOLOGY COMMITTEE WILL STILL HAVE TO RESOLVE DIFFERENCES WITH THE GOVERNMENT OPERATIONS COMMITTEE BEFORE DEBATE ON THE FLOOR. IT IS MY HOPE THAT WE CAN WORK OUT AN ACCEPTABLE VEHICLE BEFORE THAT TIME AND THAT THE RULES COMMITTEE WILL LOOK FAVORABLY UPON THE SOUND RECOMMENDATIONS SET FORTH IN THE SCIENCE COMMITTEE SUBSTITUTE AMENDMENT TO H.R. 2889.

THANK YOU.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Draft Legislative History

It is understood that section 6 of the bill requiring the submission of plans to protect computers that store sensitive data in accordance with guidelines prescribed by section 111(f) of the Federal Property and Administrative Services Act of 1949 only applies to computers subject to the provisions of that Act.

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4

[COMMITTEE PRINT]

June 3, 1986

SUBSTITUTE AMENDMENT OFFERED BY MR. GLICKMAN FOR THE SUBCOMMITTEE AMENDMENT TO H.R. 2889

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ``Computer Security Act of 1986''.

SEC. 2. PURPOSE.

(a) IN GENERAL.--The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.--The purposes of this Act are--

(1) to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines needed to assure the cost-effective security

Sanitized Copy Approved for Release 2010/12/29 : CIA-RDP87B00858R000400470016-4